Enterprise Risk

Spring 2024 / www.enterpriseriskmag.com

The official magazine of the Institute of Risk Management

IRM's risk trends 2024: IRM's groups around the globe have collaborated to provide insight into the risks organisations need to have on the radar over the next 12 months

Collaborative resilience: risk managers have a key role to play in cyber-defence / **Crisis of representation:** deepfakes are expected to pose the number-one risk over the next two years / **Improvement in action:** how to link risk management processes to the strategic direction of the organisation

Increase your earning potential with this OFQUAL accredited qualification

International Certificate in Financial Services Risk Management

Stay on top of international regulatory developments such as Solvency II and Basel III risk requirements. Study with the IRM to ensure you remain compliant and gain an understanding of how risk management impacts strategy and performance.

www.theirm.org | Tel: +44 (0)20 7709 9808 | Email: enquiries@theirm.org

irm

Enterprise Risk

Spring 2024

Editor
Arthur Piper

Produced by
Smith de Wint
Cobden Place, 5 Cobden Chambers
Pelham Street, Nottingham, NG1 2ED
Tel: +44 (0)115 958 2024
risk@sdw.co.uk
www.sdw.co.uk

Sponsorship and Advertising Sales Manager
Redactive Media
IRMsales@redactive.co.uk
Tel: +44(0)20 7324 2753

Enterprise Risk is the official publication of the Institute of Risk Management (IRM).

ISSN 2397-8848

About the IRM
The IRM is the leading professional body for Enterprise Risk Management (ERM). We drive excellence in managing risk to ensure organisations are ready for the opportunities and threats of the future. We do this by providing internationally recognised qualifications and training, publishing research and guidance, and setting professional standards.

For over 30 years our qualifications have been the global choice of qualification for risk professionals and their employers. We are a not-for-profit body, with members working in all industries, in all risk disciplines and in all sectors around the world.

Institute of Risk Management
2nd Floor, Sackville House, 143-149
Fenchurch Street, London, EC3M 6BN
Tel: +44 (0)20 7709 9808
Fax: +44 (0)20 7709 0716
enquiries@theirm.org
www.theirm.org

Copyright © 2024 Institute of Risk Management. All rights reserved. Reproduction without written permission is strictly forbidden. The views of outside contributors are not necessarily the views of IRM, its editor or its staff.

Editorial

Political manoeuvres

At the beginning of the pandemic, organisations faced the stark reality of living in an era of global supply chains. While such structures help to create the free flow of cheaper goods and products around the world, they are also fragile. As dockyard workers became sick and social distancing restrictions hit home, commercial arteries clogged up and stopped functioning.

People began speaking of deglobalisation. That involved seeking home-based suppliers for essential goods and services – or at least trying to diversify the organisation's supplier base. That trend has become particularly pronounced as political tension between the US and China has made some businesses worry about their dependency on foreign production systems.

Hard habits

The European Central Bank is sceptical about whether this is actually happening at scale. As one high-level, US risk professional told me last year, moving a factory from China to Vietnam, for instance, means giving up on 40 years of infrastructure investment surrounding that facility to a country that simply has not had the same level of industrial modernisation. And even in Russia, where many Western companies say they are committed to stop trading, most are still actively doing business. Old habits are hard to give up, it would seem.

Supply chains aside, even if organisations are beginning to deglobalise, the threats that businesses face are continuing on a global trajectory. IRM's annual risk survey (pages 10-17) shows that from cyber-risk to climate change, organisations often face different facets of the same suite of problems. There are local variations in how those trends play out, but the dimensions of those risks are familiar worldwide.

New threats

Arguably, though, it is not the familiar threats that catch the world out – but the unanticipated flare-up of some half-forgotten reality. In this case, the emergence of a new Cold-War divide between the US and Europe, on the one hand, and Russia and China on the other. Just as few expected Russia to invade Ukraine, fewer still believed that the country's economy would weather the blizzard of sanctions levelled at it.

But even if this scenario does come about, it would be a mistake to believe that this Cold War would be anything like the last one. For a start, the inter-relations between China and the rest of the world are deep and likely abiding. What the US seems to wish is that something could put a brake on China's advancing technological capabilities – at the same time as retaining the ability to depend on it as a key trading partner. It is not clear that approach can succeed.

It is not surprising, then, that so much debate in this year's IRM survey centres around the word "political".

Arthur Piper
Editor

irm
Developing risk professionals

THE INSTITUTE OF OPERATIONAL RISK

MIX
Paper from responsible sources
FSC® C017177
FSC www.fsc.org

Delivered to meet your companies culture and work priorities

Scan me!

In-House Training

We spend time with you to identify and assess your specific training needs to ensure we develop a course that meets all of your objectives.

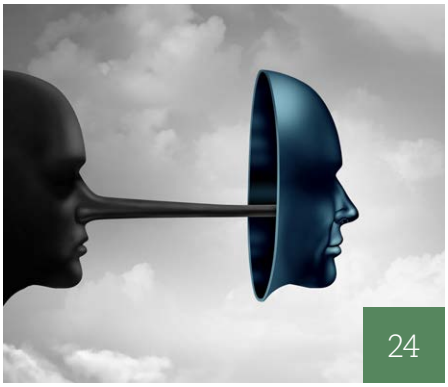
www.theirm.org | Tel: +44 (0)7469 353441 | Email: joanna.kraska@theirm.org

irm

Contents

10

18


24

30

Features

10 IRM's risk trends 2024
IRM's groups around the globe have collaborated to provide insight into the risks organisations need to have on the radar over the next 12 months

18 Collaborative resilience
Cyber-risk is frequently cited by businesses as their greatest threat. Risk managers have a vital role to play in bringing people in the organisation together to meet the challenge proactively

24 Crisis of representation
Deepfakes are expected to pose the number-one risk globally over the next two years, but regulation is moving much more slowly than the technology

30 Improvement in action
Risk professionals are meant to enhance their processes and link them to the strategic direction of the business. But what does that mean in practice?

REGULARS

7 IRM Viewpoint
IRM has strengthened the expertise of its global board with three new appointments

8 Trending
The stories and news affecting the wider business environment as interpreted by our infographics team

36 Directory
In need of insurance services, risk management software and solutions, or training? Look no further than our listings

38 Toffler
As work becomes increasingly infected with pointless activities, organisations need to act to improve worker engagement

IRM Advisory Services Ltd

IRM Advisory

Advice, Guidance and Mentoring

Level up your risk performance

IRM Advisory will advise, guide and mentor you in levelling up your risk performance by helping you get the most out of your risk frameworks and programs.

From understanding your risk appetite to setting the proper risk levels and developing an enterprise-wide risk culture.

Scan me!

hub.theirm.org/advisory

advisory@theirm.org

Global board boost

IRM has strengthened the expertise of its global board with three new appointments

Dorothy Maseke, CFIRM, has been appointed as the new joint deputy chair of the IRM Global Board. Mariam Crichton and Esther Chesterman are new independent directors.

Maseke brings a wealth of experience to her new role, having previously served on the IRM Global Board as director and chair of the investment committee. She is the founder of the IRM East Africa Regional Group, where her leadership has been instrumental in fostering the growth of IRM throughout the continent.

Internationalisation

Maseke is also spearheading the establishment of a registered professional body in Africa, which will support IRM's internationalisation strategy. That will include value-adding activities in Africa, for example, through the development of commercial products and strategic partnerships.

She also chairs IRM's nominations committee. Maseke is currently a nature finance specialist, championing impactful nature and biodiversity initiatives that foster sustainable development and strategic investments across diverse African landscapes.

Dorothy's accomplishments have garnered recognition, including being named one of the Top 40 Under 40 Women in Kenya and one of the Top 50 Women in Insurance in Africa in 2022. Her multifaceted skills and passion for development and investment in Africa will undoubtedly enrich the IRM Global Board's strategic initiatives.

Independent directors

Crichton is one of two new appointees to the IRM Board as an independent director and has been the driving force behind the growth of numerous tech startups – either as a board member or CEO. Her career has been dedicated to delivering global technology solutions that make a positive environmental and social impact, particularly in the realms of geospatial and international development.

The other is Chesterman, who has also been appointed chair of the awarding committee. This committee will provide IRM's board with assurance that IRM remains compliant with the general condition of recognition as stipulated by Ofqual as well as driving the development of new and regulated qualifications.

Chesterman has worked in education for over 25 years, initially as co-owner of an independent training provider, The Profile Partnership. In 2017, she became general manager of NCC Education, a UK awarding body offering qualifications globally. Since April 2021, Chesterman has been CEO of the National Extension College, a not-for-profit organisation for distance learning, making education more accessible to those unable to study in a mainstream school/college.

Wealth of experience

Stephen Sidebottom, chair of IRM, said, "we are thrilled to appoint Dorothy Maseke as joint-deputy chair and also welcome Mariam and Esther to our Board."

"Their wealth of experience and diverse perspectives will be invaluable as we continue to navigate the complexities of risk management in an ever-evolving landscape. These appointments underscore our dedication to fostering leadership that drives innovation and resilience in today's dynamic business environment, for the benefit of the institute and wider business and society."

"Their wealth of experience and diverse perspectives will be invaluable as we continue to navigate the complexities of risk management in an ever-evolving landscape

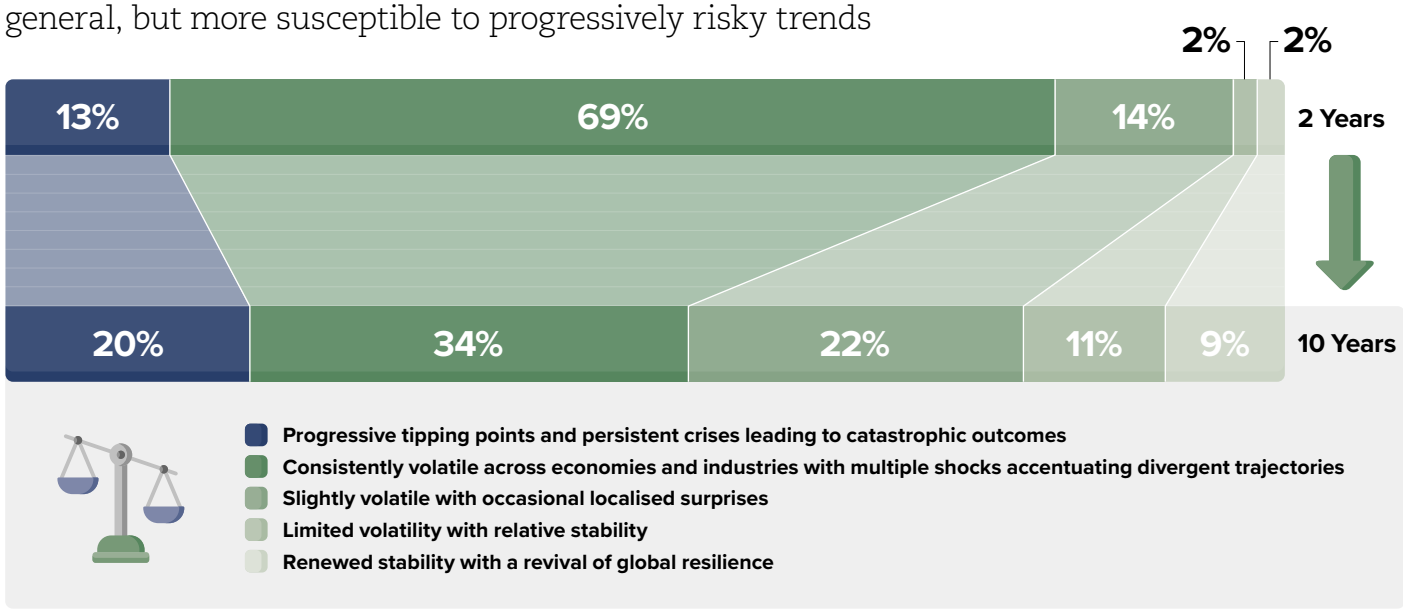
Trending

DATA

The latest stories and news affecting the wider business environment as interpreted by our infographics team

Potential "tipping points" for catastrophe increasing

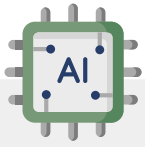
In ten years' time, the risk landscape may be less volatile in general, but more susceptible to progressively risky trends



Source: *World Economic Forum, Global Risks Perception Survey 2022-2023*

AI looms as compliance risk

Proportion of compliance professionals in financial firms who say they struggle to comply with evolving regulations today



57%
The accelerated use of AI

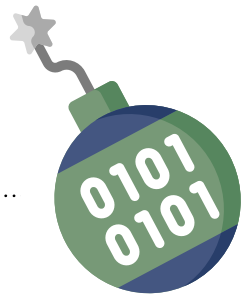
56%
Global economic instability

40%
Digital assets and crypto markets

30%
The geopolitical situation

Source: *eflow, Global trends in market abuse and trade surveillance*

Executives become increasingly concerned over digital disruption by 2034



Over the next ten years, executives expect talent and digital risks to predominate

Top 5 risks for 2024

1	Economic conditions including inflationary pressures	5.96
2	Ability to attract, develop and retain top talent, manage shifts in labor expectations, and address succession challenges	5.93
3	Cyber threats	5.90
4	Third-party risks	5.63
5	Heightened regulatory changes and scrutiny	5.61

Top 5 risks for 2034

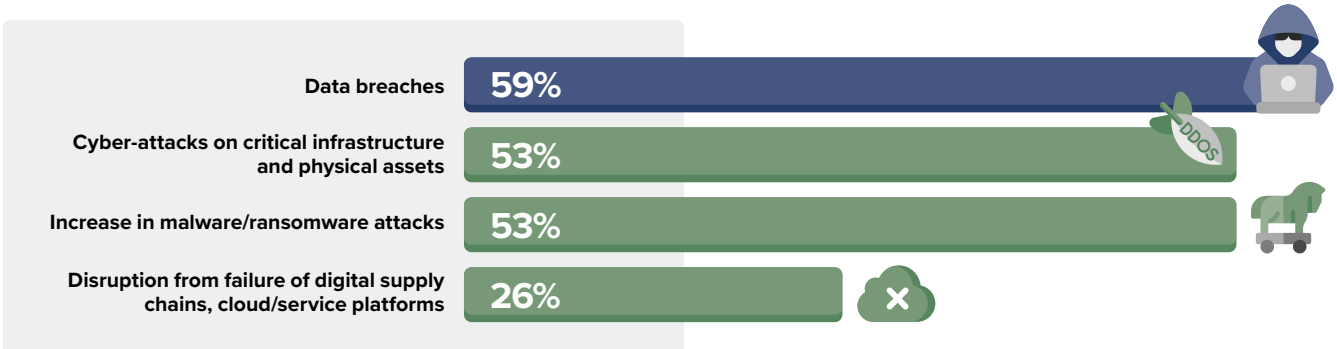
1	Cyber threats	6.44
2	Ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges	6.27
3	Adoption of digital technologies requiring new skills in short supply	6.16
4	Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces	6.15
5	Heightened regulatory changes and scrutiny	6.13

- Risks with an average score of 6.0 or higher are classified as having a “significant impact” over the next 12 months (2024)/over the next decade (2034).
- Risks with an average score of 4.51 through 5.99 are classified as having a “potential impact” over the next 12 months (2024)/over the next decade (2034).

Source: *Protiviti.com, Executive Perspectives on Top Risks for 2024 and a Decade Later*

Data breaches top 2024 cyber worry list

Cyber risk is seen by executives as the top risk globally with data breaches the main concern



Source: *Allianz Risk Barometer 2024*

IRM's risk trends 2024

IRM's groups around the globe have collaborated to provide insight into the risks organisations need to have on the radar over the next 12 months

People risk

From a cost-of-living crisis to a renewed focus on mental well-being, people will move more centre stage over the coming year

Many sectors and regions have identified people risk as being a number-one priority following the pandemic and the continuing cost-of-living crisis in many countries. For example, charities have identified people-related risks as the most significant for the sector as they reflect on 2023 and move into 2024. The effects of the pandemic and the focus on organisation recovery has taken its toll on staff wellbeing as workforces have been working at pace and have been under pressure to deliver services, often in challenging and stressful circumstances.

This led to high reports of burnout, people leaving the organisation and difficulty in recruiting and retaining to key roles. This requires the sector to prioritise the wellbeing and mental health of its workforce and to provide effective support and resources.

The risk around the workforce has been exacerbated further by the changing landscape of volunteering, which has seen a demographic shift of available volunteers where people have changed working patterns with shifting responsibilities. Charities must review their approaches to volunteering and offer more flexible roles to continue to provide a strong volunteering offer and support the delivery of charitable missions.

Charity risk surveys have indicated a growing risk from increased management and running costs that are significantly impacting budget. Charities are looking to modify and adapt their existing delivery models to pursue new and creative ways to deliver their strategic objectives.

As of April 2023, Australian federal legislation has mandated that workplaces need to manage psychosocial hazards under the Work Health and Safety Act (WHS Act). The drivers of psychosocial risk management are the $12.8 billion cost of mental ill-health to the Australian Workplace (2023 Deloitte Risk Advisory).

> **“ The effects of the pandemic and the focus on organisation recovery has taken its toll on staff wellbeing**

There is an accelerating cost of psychosocial hazards, which are the aspects of work or the work environment that have the potential to increase the risk of work-related stress, with further potential to lead to psychological or physical harm.

Examples include job-related hazards (for example, job demands, conflict in the workplace), organisational process hazards (for example, poor change management or recognition), harmful behaviour hazards (for example, bullying, harassment, discrimination) and safety culture hazards (for example, fatigue, poor physical work environment). In the health and education sector in Australia we have seen a trend towards worker fatigue and disengagement.

There is a trend of mental health deterioration at the population level through increased observation of burnout (68.5 per cent of Australian workers) and general mental disorder prevalence leading to decreased productivity and workforce participation outcomes. The status of psychosocial risk codes of practice in Australia is five of eight jurisdictions (including the Commonwealth) have regulations dealing with psychosocial risk in force. We anticipate that just as most jurisdictions have released codes of practice for managing psychosocial hazards, most employers will begin to implement mitigative measures to decrease the threat of psychosocial hazards to their employees.

IRM Charities Group.
IRM Australia Group.

Technology and innovation

Bitcoin could gain widespread adoption in 2024, but advances in generative AI need careful handling

The widespread understanding and adoption of Bitcoin is expected to gain momentum during 2024, driven by increasing institutional interest and regulatory clarity in various jurisdictions. In particular, the approval of a spot Bitcoin Exchange Traded Fund in the US is expected to provide the necessary signal to the traditional financial sector that Bitcoin is an accepted vehicle for investment.

The continued improvements in energy efficiency and its use to drive renewable energy could address some of the environmental concerns associated with Bitcoin, potentially mitigating criticisms and attracting a broader user base. As more traditional financial players integrate Bitcoin into their portfolios, the market could witness a significant increase of investment, leading to increased stability and reduced volatility compared to previous years. That being said, we can expect a significant rise in price from current levels.

However, challenges may persist, such as ongoing regulatory developments and potential geopolitical factors that could impact the global cryptocurrency landscape. The introduction of Central Bank Digital Currencies (CBDCs) indicates that countries are keen to keep digital currencies centralised, which indicates that perhaps restrictive regulations could be introduced with regard to the use of Bitcoin.

If Bitcoin manages to navigate these challenges successfully, however, 2024 may see it solidify its position as not only a digital gold but also a crucial component of the evolving financial landscape, paving the way for further innovation and integration within the broader economy.

Advances in generative artificial intelligence over the past 12 months is a good reminder that risk managers must be aware of our risk appetite and how to balance both threats and opportunities. Ethical considerations in this area are still somehow blurry and inconclusive.

Although AI can lead to significant advancements in medicine, business, trading, monitoring, surveillance and farming, etc, there has been an ongoing fear of its effects, for instance, in unemployment and social security. Numerous unanswered questions regarding who is in control of this technology, who benefits and who loses from it are still to be tackled by broader risk management and interdisciplinary communities.

IRM Innovation Group, with technology insights from Alex Larsen and Dylan Campbell.

> **The continued improvements in energy efficiency and its use to drive renewable energy could address some of the environmental concerns associated with Bitcoin**

Tackling real issues

Instead of simply looking at reporting on ESG, risk managers can help support meaningful initiatives in their organisations

Environmental and Social Governance – ESG, or rather the letters E, S and G – were a topic of discussion in 2023. But, as predicted, much dialogue focused on reporting rather than the substance of sustainable development.

Risk professionals have a role in supporting the leadership of organisations to set out their vision of what sustainable development means for their organisations as well as proactively acting upon strategies for its realisation. The nature of changes in the external environment will present further pressures on organisations to be transparent and accountable to a wider array of stakeholders, including in addressing risks related to modern slavery, equality, diversity, inclusion, safeguarding, security, health, safety and welfare as well as the natural environment.

Those in leadership positions will continue to be scrutinised in real time, notably on social media, for the way in which they behave and run their organisations. In this context, meeting stakeholders' expectations including increasingly demanding disclosure requirements will see organisations achieve greater levels of transparency for investors than ever before and provide clarity over their exposure, as well as identify opportunities including in relation to climate change. ESG should be seen and acted upon as a platform for sustainable development aligned with long-term value creation in the context of behaving in an ethical and sustainable manner.

The risk professional is well placed to assist the governing body in this regard by supporting the management of environmental and social matters associated with global challenges. Failure to address such risks will present further sustainable development challenges for the international community and international organisations, notably in relation to increasing numbers of people migrating or finding themselves in poverty and therefore at risk of modern slavery; modern slavery, notably the use of child labour, is a matter of concern for the leadership of purpose-driven organisations and the IRM ESG Group.

Risk professionals have a role in supporting the leadership of organisations to set out their vision of what sustainable development means for their organisations

IRM Environmental and Social Governance Group.

Focus on nature

Regulation turns to nature and greenwashing

The Taskforce on Nature-related Financial Disclosures (TNFD) is one of many globally backed initiatives that provides holistic practical recommendations to enable the first steps of standardising this currently complicated challenge. TNFD provides guidance on the identification and assessment of nature-related issues. They suggest using an integrated assessment approach called the LEAP approach which stands for (Locate, Evaluate, Assess and Prepare).

Understanding nature refers to the natural world, emphasising the diversity of living organisms, including people, and their interactions with each other and their environment. It is made up of four realms: land, ocean, freshwater and atmosphere.

While broad, the TNFD's most recent suite of 14 key recommendations lean towards helping organisations cut through the complexity of metrics and indicators available, permitting the use of carefully selected proxy data and analysis. Simplifying this process will help to inform required sustainable governance and short-, medium- and long-term risk and opportunity strategy management through an annually comparable reporting format.

With respect to the assessment process, it is important to recognise new innovative approaches that are available, such as use of satellite imagery, that offer accessible insights for decision-makers in green finance and corporate reporting.

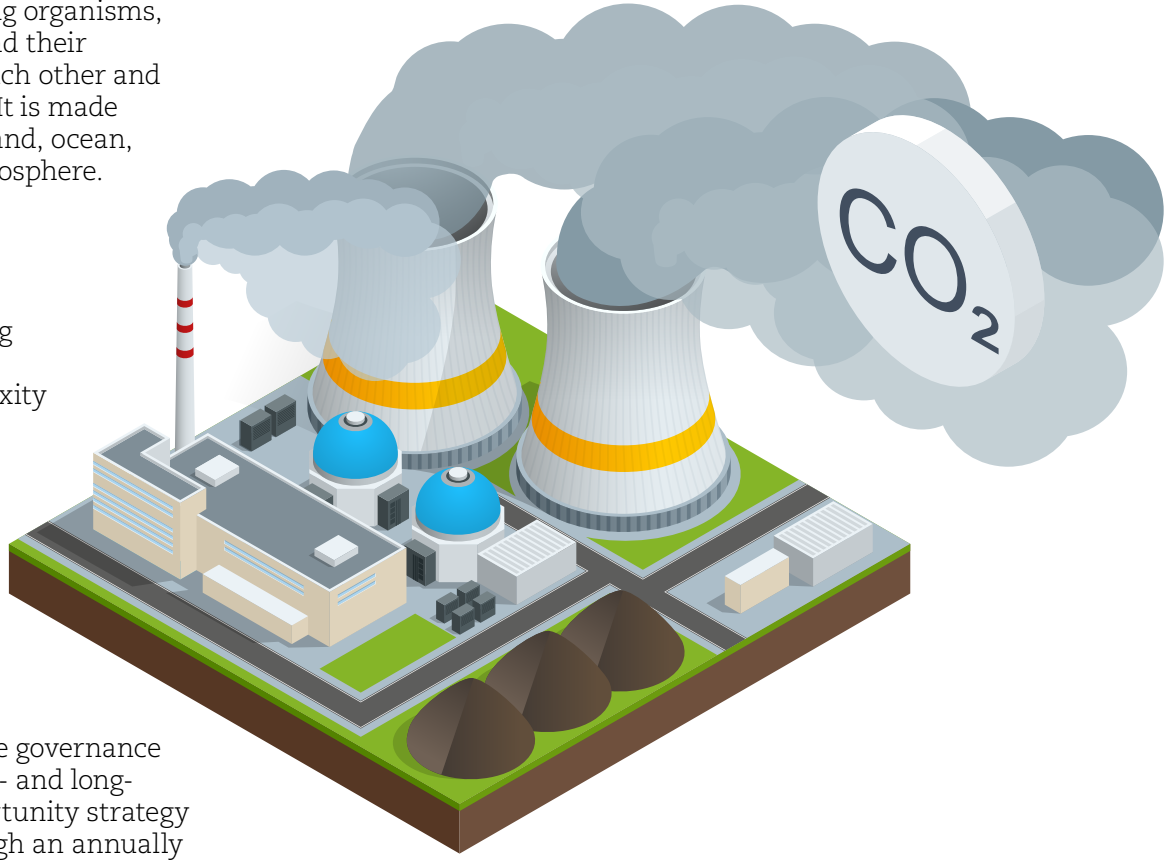
Greenwashing, or indeed the efforts by firms to present themselves in a favourable public light through association, is not a new concept and one that we discussed in last year's report.

However, it is the increasing regulatory enforcement that is the main global trend. While governments remain the main targets, the number of cases filed against corporates has increased, and the range of sectors targeted has become more diverse, moving to include food, agriculture, transport and finance as well as the core cases against oil and gas companies.

This reflects the increasing number of complaints and legal cases that have also been brought on climate change grounds. Specific examples include disinformation spread by high-emitting companies about the impacts of their products.

IRM Climate Change Group.

> **TNFD's most recent suite of 14 key recommendations lean towards helping organisations cut through the complexity of metrics and indicators available**



Rule changes fuel tighter controls

Interest rates and higher borrowing costs are affecting both financial institutions and infrastructure businesses

A high inflation regime that started in 2021 caused by the emergency of the pandemic and geopolitical conflicts led central banks to raise interest rates gradually in order to meet targets. Banks benefited from higher returns under high interest rate regimes; however, the returns can easily be offset by rising defaults in a squeezed credit market over time. Interest rates have started a downward trend giving the hope that defaults will not be as acute and financial institutions can portfolio strategies. It remains uncertain whether the drop will be sustained.

The failure of the global systemically important bank (G-SIB) Credit Suisse in the first quarter of 2023 as a result of runs on the bank shows the importance of a strong resolution framework supported by strong enterprise risk management. Financial institutions need to ensure that regulators have confidence in the strength of their operations. While they are complex, real-time risk assessments can be a solution by taking advantage of the advancement in technology.

In fact, changes to financial processes and regulations are an area of risk and opportunity for the infrastructure sector; current regulations will likely lead to increased capital charges for infrastructure, making the sector less attractive to investment. A KPMG report references upwards of 7 per cent of global GDP between now and 2050 is what it will take to meet climate change targets.

There is a visible divide in the type of projects which attract public and private investment: central governments are investing heavily in transport projects, whereas private investors are targeting renewable projects, which receive half of all private sector investment in infrastructure.

This is expected to continue into 2024, with greater focus on ESG within infrastructure projects. The sector already does well in this area, in comparison with other sectors, so there could be an opportunity to attract more private investment in other subsectors beyond renewables. For example, developing a standardised method to verify how green an investment is could be a key to unlocking some of this capital.

> **Central governments are investing heavily in transport projects, whereas private investors are targeting renewable projects**

IRM Financial Services Group.
IRM Infrastructure Risk Group.

The politics of energy

A mixture of politics and policies could dominate the coming 12 months

1. Geopolitical concerns

Geopolitical tensions in the Middle East could disrupt oil supplies, putting upward pressure on prices if we see an escalation of the current unrest in the region.

2. Asian geopolitical and macroeconomic shifts

Companies such as the Chinese property group Evergrande (given its recent crisis) is an indicator to watch given that fears are rising about its ability to repay a cascading pile of debt against the backdrop of muted property sales and rising interest rates in mainland China. This issue is linked to efforts by Beijing to rein in the property sector in the past year. We expect the effect of long-term interest rates to have a significant impact on this over-extended indebted corporation – and others could follow.

3. Political effects on critical supply chains

Supply chains will face a squeeze. Political moves in particular could impact the availability of critical minerals needed for the drive towards electrification, which will weigh heavily on the direction of renewables and alternative energy.

4. Ongoing changes in the EU energy market

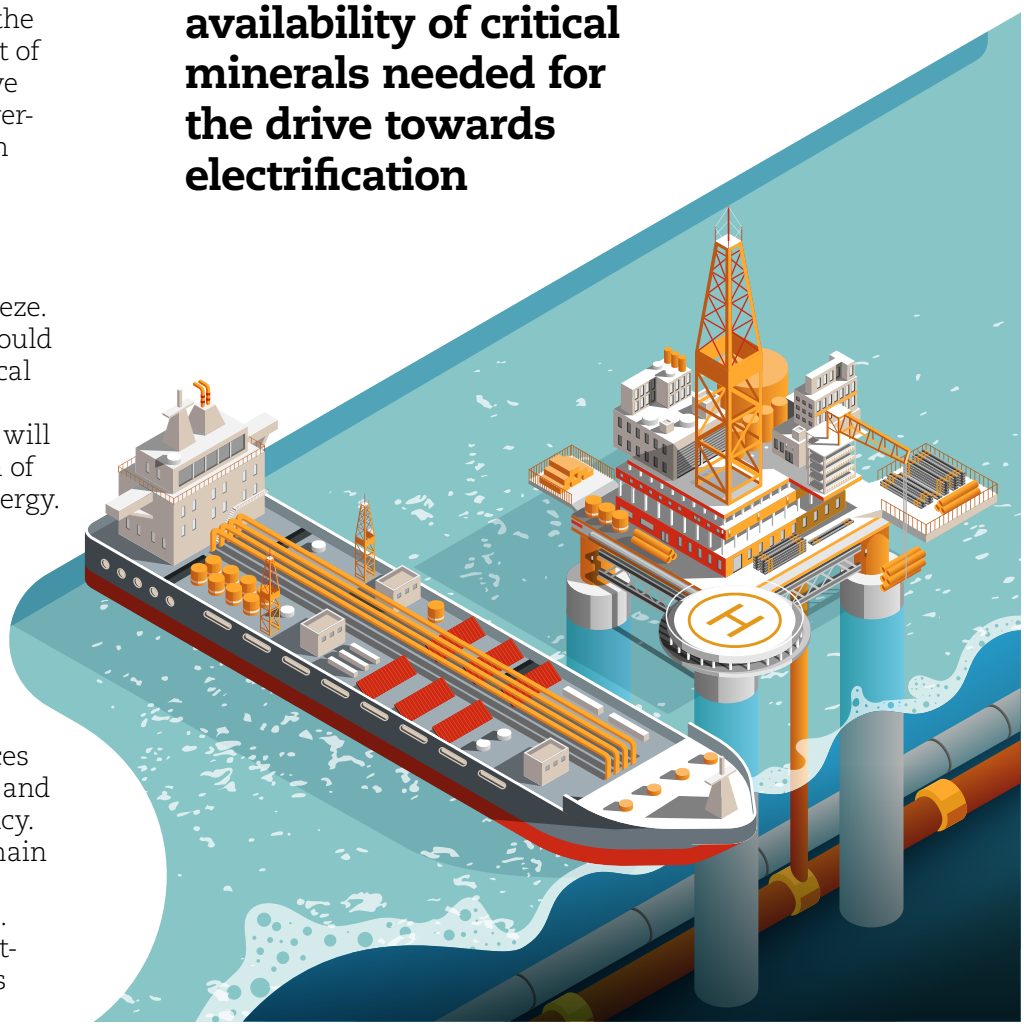
There is a mix of issues relating to energy generation and aims to achieve stable prices against a backdrop of volatile fuel prices – all driven by ongoing unrest and a lack of clarity on energy policy. Coal and other fossil fuels remain firmly in the mix, threatening the ambitious net-zero targets. As we witnessed last year, cost-of-living and societal demands will also influence policy.

5. Backsliding on renewable energy and the drive for sustainability

The underlying suspicion of renewables and their much higher costs will shift policy on energy towards retaining and potentially increasing the mix of more traditional and affordable sources of energy. These policy shifts will be driven by higher levels of pressure falling on political leaders coming from citizens exercising their voices at the ballot box. This renewed democratisation will favour greater consideration being given to addressing the economic and societal elements of energy policy at the expense of green imperatives.

IRM Energy & Renewables Group.

Political moves could impact the availability of critical minerals needed for the drive towards electrification



TOP FIVE RISKS AFFECTING INDIA

- **Cybersecurity threats:** The increasing digitisation of Indian businesses makes them susceptible to cyber-threats, including data breaches and ransomware attacks.
- **Geopolitical tensions:** India's geopolitical landscape introduces risks related to border tensions, trade disruptions and diplomatic challenges.
- **Climate change and environmental risks:** Given India's vulnerability to climate change, environmental risks such as extreme weather events and resource scarcity are significant concerns.
- **Economic uncertainties:** Fluctuations in the global and domestic economy, exacerbated by factors like inflation and currency depreciation, present economic risks.
- **Regulatory changes:** Rapid shifts in regulatory frameworks, particularly in response to ESG considerations, pose compliance challenges for businesses operating in India.

IRM's Interest Groups

Join risk professionals from around the world and help IRM set the agenda on risk

Special Interest Groups

IRM's special interest groups (SIGs) provide members with specific forums to network, exchange views and share best practice with their peers. Joining a group enables you to:

- Make valuable contacts and gain insight into topical, relevant and challenging risk issues
- Further develop your knowledge in specialist areas
- Apply your additional knowledge and new contacts to drive improvement in your business' performance and raise the profile of risk management within it

Members can join as many groups as they like. Non-members can join our groups for a limited period of time, but will need to become an IRM member if they wish to continue attending meetings and enjoy wider membership benefits.

Regional Groups

Aim to:

- Develop member knowledge
- Encourage discussion and add value to the risk profession
- Expand the boundaries of risk management thinking
- Encourage growth in IRM's community

Members are free to join as many groups as they like. We regularly send all members information about their local group. Non-members can attend a group for a limited period of time but will need to join the IRM if they wish to continue attending these meetings and receive wider membership benefits.

GET INVOLVED

DOWNLOAD IRM'S RISK TRENDS 2024 SURVEY HERE

Collaborative resilience

BY CATHERINE NYAGA-MBITHI

Cyber-risk is frequently cited by businesses as their greatest threat. Risk managers have a vital role to play in bringing people in the organisation together to meet the challenge proactively

One sunny Thursday afternoon, Sylvia Wanjiru, a 34-year-old trader managing a second-hand clothing business in Riruta Satellite, a bustling suburb west of Nairobi, Kenya's capital city, found herself unexpectedly confronted with a distressing call. The voice on the other end, purportedly that of a teacher from her son's school, was urgently requesting immediate monetary assistance for Sylvia's son's emergency medical treatment after a fall while playing in school. Overwhelmed by concern for her child, Sylvia was on the verge of complying with the request when her fellow traders, seizing on the situation, quizzed the caller, who then failed to give a fair description of the son, and quickly disconnected the call.

Sylvia's discerning troubles reflect an emerging trend where sensitive customer data – including names, phone numbers and financial information – is obtained illegally through collusion between cybercriminals and money-transfer bureau attendants, offering cash in exchange for the information. This shows a glaring vulnerability within the system, where unsuspecting individuals unknowingly expose themselves to exploitation when performing routine transactions.

Range of attacks

Though most of these types of social engineering attacks, phishing scams and business email compromise go unreported, they reflect a growing trend of increasingly sophisticated and bolder deceptions. In a recent well-publicised case, Brian Mwenda manipulated information from

> **Unsuspecting individuals unknowingly expose themselves to exploitation when performing routine transactions**

the Law Society of Kenya (LSK) – the professional body overseeing legal practice in Kenya – to enable him to successfully defend cases in court under a false identity.

In addition, Africa, particularly Kenya, has witnessed a surge in ransomware attacks targeting companies of all sizes. According to the Cybersecurity Report for October to December 2023 by the Communications Authority of Kenya (CAK), there was a significant increase in cyber-threat events during this period, reaching 1.2 billion, marking a staggering 943 per cent rise from the previous quarter's 123 million.

Another type of threat that has emerged prominently is Advanced Persistent Threats (APTs). These threats, often state-sponsored, infiltrate computer networks and remain undetected for extended periods. Recent examples include apparent backdoor diplomacy by Chinese actors and the actions of the self-styled Russian hacker group "Anonymous Sudan", which engaged in Distributed Denial of Service (DDoS) (*3) attacks in 2023, rendering key government services inaccessible online.

Supply chain attacks have also increased that involve the compromise of software or hardware of trusted vendors and suppliers to gain unauthorised access to targeted businesses. Attackers also target third-party service providers to gain widespread access to multiple organisations. Further, as most organisations move to the cloud, so do the associated security risks. Companies will face challenges such as misconfigurations, insecure Application Programming Interface (API)s and data breaches in cloud platforms. As the number of connected devices increases, so does potential attacks for criminals. Internet of Things (IoT) devices are targeted more frequently due to often inadequate security measures. According to the Serianu, Africa Cybersecurity Report 2023, IoT malware cases increased by 87 per cent in the year 2022 from 2021 closing at 112.3 million cases.

Maturity levels

Different organisations are at different levels of maturity when it comes to management of cyber-risks. Some of the notable actions implemented by some enterprises include, first, the adoption of zero-trust security frameworks to mitigate "insider threats" and "lateral movement". Trust is not a control. All users inside and outside an organisation's network must be authenticated, authorised and continuously validated for security configuration and posture before being granted (or keeping access) to applications and data.

Second, they are continuously training employees. Organisations should recognise that employees are the weakest link in dealing with cyber-threats. Employees should be reminded of their responsibilities, such as recognising and reporting suspicious activities that they may come across in the course of their work. Employees are encouraged to keep abreast of developments within the industry from their peers through the various industry forums, such as the Information Systems Audit and Control Association (ISACA).

Third, they are adopting multifactor authentication (MFA) and strong encryption protocols to secure data in sensitive systems. This refers to the use of two or more distinct instances of the three factors of authentication (something you know, something you have, something you are) for identity verification. Examples include having a password, a token number and a fingerprint respectively for identity verification before granting access to any system.

Finally, organisations are also enforcing compliance with industry regulations and standards to help with the mitigation of risks arising from cyber-threats. Some of the notable regulations are the European Union General Data Protection Regulation (EU-GDPR), the Kenya Data Protection Act (2019) and the Cybersecurity Guidelines issued by Central Bank of Kenya (CBK) in 2018. The International Organization for Standardization (ISO) 27001 Information Security Management Systems provides the minimum requirements for an effective information security management system.

Organisations are also enforcing compliance with industry regulations and standards to help with the mitigation of risks arising from cyber-threats

Challenges

But organisations still face major challenges in dealing with the threat. For example, there is a lack of appropriate cybersecurity competencies at board level. The board sets the tone at the top in management of the cyber-risks. Without the right competencies, the board cannot provide the required oversight leading to failure in cyber-risk management. In addition, the budget to implement the controls may be out of reach for most organisations – especially in areas such as the real-time monitoring of potential threats. Organisations should consider their risk appetite in determining how to allocate resources in mitigating cyber-risks.

Staff members may lack

integrity and, therefore, as much as training is conducted, they may still perpetrate some of these vices. For that reason, it is important to have robust human resource policies and procedures clearly identifying staff vetting at onboarding and disciplinary procedures for lack of integrity. In fact, most employees think that the responsibility of managing cyber-risks is for the Information Technology (IT) business unit, a concept known as "silo mentality". Organisations must ensure that all employees are aware of their responsibility in managing cyber-risks on an ongoing basis.

Most organisations, especially the Small and Medium-sized Enterprises (SMEs) do not have appropriately skilled cybersecurity professionals to manage cyber-risks. Such organisations should consider outsourcing the cyber-risk management programme to a consultant. Further, scalability of current technology solutions for SMEs may pose challenges due to factors such as limited resources, outdated or inadequate technology, risk management concerns and the necessity to ensure compliance with diverse regulations. While scalability is desirable, it can present a notable challenge for organisations.

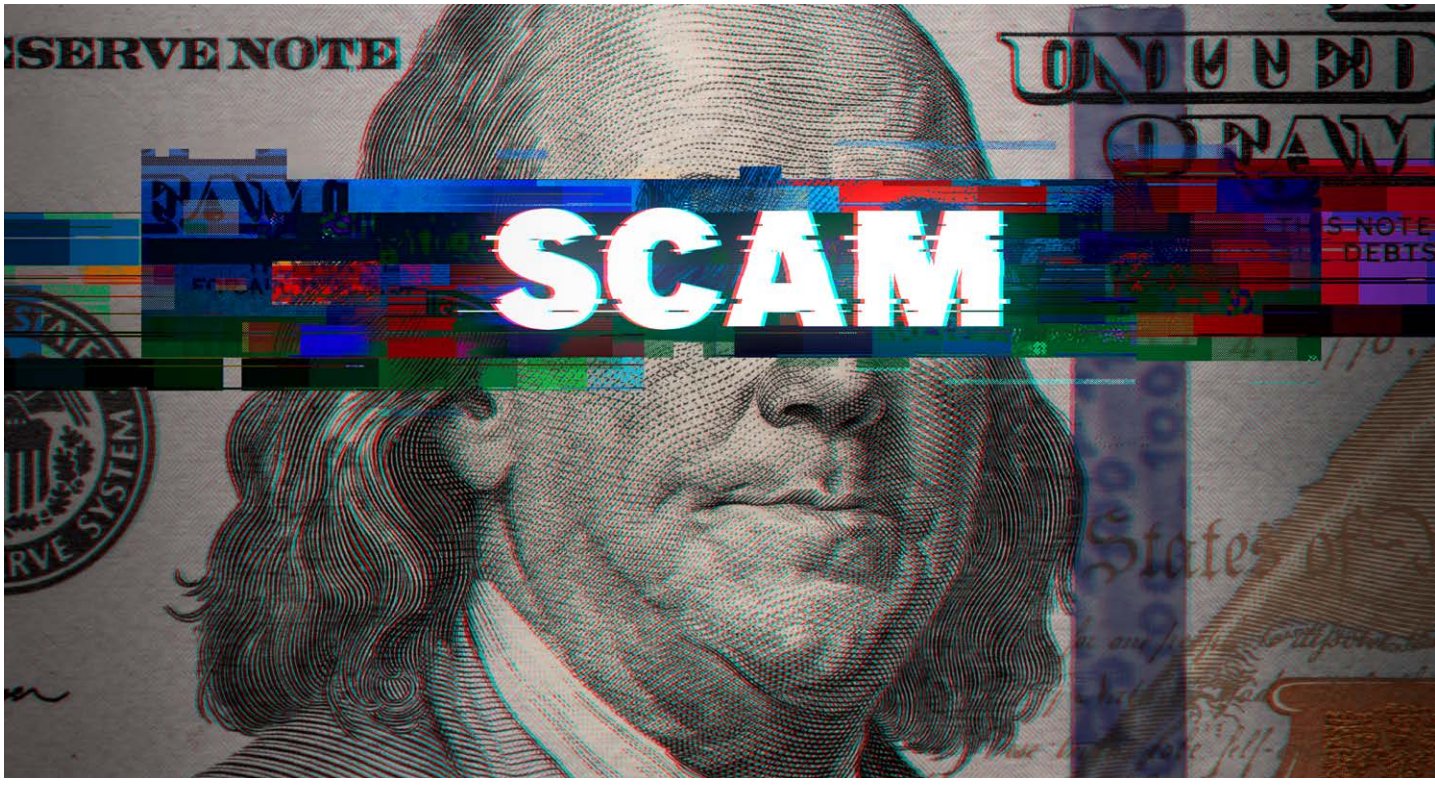
> **There is a lack of appropriate cybersecurity competencies at board level**

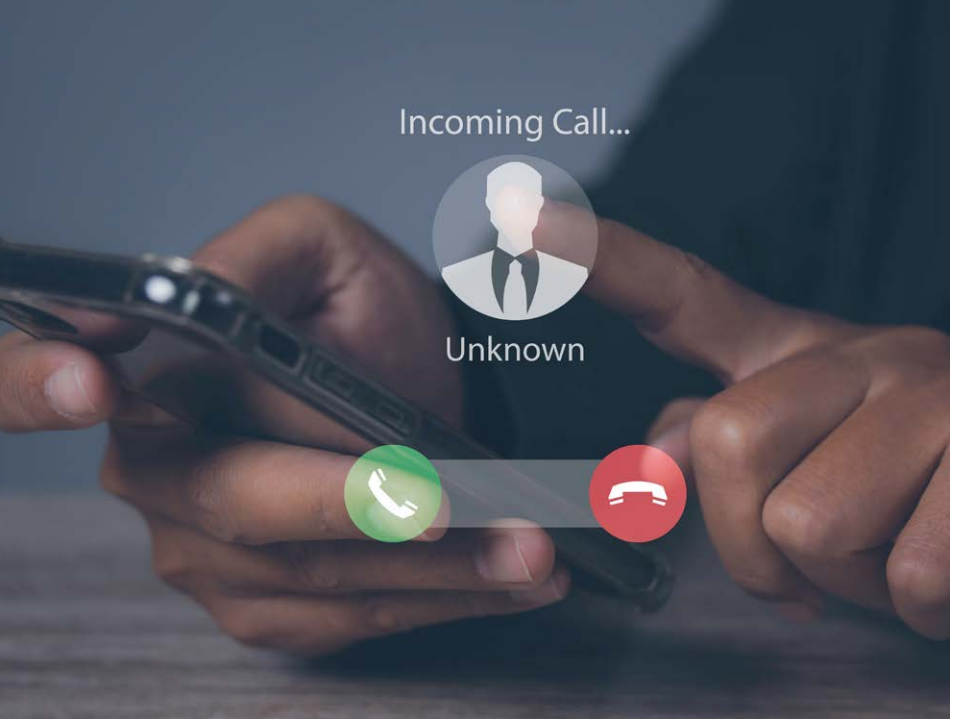
The fact that the threat landscape has been evolving rapidly has made it more difficult for cyber-risk professionals to deal with the risks effectively. In addition, vulnerabilities from remote working following the COVID-19 pandemic have increased significantly. Organisations should ensure that there are adequate security measures for remote working and have robust disaster recovery plans in place.

Risk management's role

A risk manager has a key role in assisting businesses to deal with cyber-risks. For example, risk management can recommend an enhancement of the board's cybersecurity competencies and oversight capabilities. Since the board sets the tone for cyber-risk management, and approves policies and procedures that guide the risk management efforts, the board should include a member with relevant IT and cybersecurity knowledge. That will enable the governance body to discharge their fiduciary responsibilities in cyber-risk management.

Organisations also need to build and enhance threat detection and response capabilities through automation. Risk managers can get threat alerts on a real-time basis, such as the location that the threats happened, to enable them to make decisions quickly. Regular vulnerability assessments and penetration testing should focus on both identifying and remediating risk. Risk managers should continuously monitor security controls and configurations. In addition, they should develop cyber-risk frameworks which are





> **With the right understanding of the organisational cyber-risks, the board will offer a more effective oversight over cybersecurity threats**

risk based and guided by threat exposures identified through a cyber-risk assessment.

Getting the entire organisation on board is crucial. Risk managers can position cybersecurity as a business-value creation driver for internal teams. Teams may have a negative perception towards the cyber-risk management efforts leading to laxity in implementation. Risk managers should constantly communicate the value of these efforts to all the stakeholders within the organisation. That is why it is important for risk managers to move from a policing mindset to one that promotes an integrated, comprehensive cyber-strategy powered by people, processes and technology.

Encouraging a collaborative approach in risk management through decentralising cybersecurity management and involving non-technical business departments is also important. Cyber-risk management is the responsibility of all and not just the risk manager/IT. The risk manager should develop regular refresher training to remind staff of their responsibilities.

Since organisations are not able to stop all cyber-related attacks, risk managers should have in place an incident management process to respond to a service interruption and restore the service to its operational state. They should also institute controls to prevent recurrence of the issue.

As part of responding to cyber-risks, an organisation could opt to transfer the risk to an insurance company through obtaining cyber-insurance policies.

It is vital to remember to ensure that third parties' (supply chains') systems are protected. In a recent survey conducted by KPMG, out of 1,325 CEOs interviewed, 76 per cent believed that protecting their partner ecosystem and supply chain is just as essential as building their own security infrastructure.

Better resilience

Risk management efforts play a critical role in enhancing the resilience of an organisation. Several key factors contribute to the positive impact of risk management on resilience.

First, with the right understanding of the organisational cyber-risks, the board will offer a more effective oversight over cybersecurity threats. The board's involvement fosters a culture of risk consciousness throughout the organisation, promoting preparedness and agility in dealing with risks.

Second, an improvement in organisational risk culture is vital for building better resilience.

Management view risk as an enabler in decision-making at both strategic and operational levels.

Furthermore, collaboration in risk management is crucial for identifying and addressing emerging risks comprehensively. It allows for the sharing of perspectives and expertise, leading to more effective risk mitigation strategies.

By prioritising risks, organisations can allocate resources more effectively, that is, to investments that will manage the cyber-threats within the risk appetite. Moreover, effective risk management can result in reduced insurance premiums leading to significant cost savings for the organisation.

Finally, risk management efforts can also enhance working relationships with suppliers. By assessing the vulnerabilities of the connections with suppliers, they can help them to improve the exposures to their systems and other clients to whom they are providing services.

Catherine Nyaga-Mbithi is co-chair of IRM's East Africa Group and internal audit manager at ABSA Life Assurance Kenya.

Supercharge your career with this OFQUAL accreditation!

International Certificate in Enterprise Risk Management

Risk is part of every business, from the pandemic-to cyber threats-to supply chain disruptions. Study with the IRM to improve your career and earning potential by gaining a solid foundation in the theory and practice of effective risk management.

Scan me!

www.theirm.org | Tel: +44 (0)20 7709 9808 | Email: enquiries@theirm.org

irm

Crisis of representation

BY ARTHUR PIPER

Deepfakes are expected to pose the number-one risk globally over the next two years, but regulation is moving much more slowly than the technology

US President Joe Biden recently called several thousand voters in New Hampshire to tell them that he needed their help in defeating his Republican opponents in elections to be held in November. Urging potential Democrat supporters to not waste their votes on an election in January 2024, he seemed to imply that they could cast their votes in only one of the forthcoming elections in the state that year.

Except it was not President Biden on the phone. The state's Attorney General's Office was quick to launch an investigation. "These messages appear to be an unlawful attempt to disrupt the New Hampshire Presidential Primary Election and to suppress New Hampshire voters," it said in a statement. "New Hampshire voters should disregard the content of this message entirely. Voting in the New Hampshire Presidential Primary Election does not preclude a voter from additionally voting in the November General Election."

Socially divisive

By February, the Attorney General's Office had issued cease-and-desist orders against two Texas companies it believed had used AI-powered technology to create the bogus voice on the calls. No doubt the investigation will take time to unravel, but with an estimated three billion people going to electoral polls over the next two years, the World Economic Forum (WEF) said that such tactics pose a major threat to political stability.

"Emerging as the most severe global risk anticipated over the next two years, foreign and domestic actors alike will leverage misinformation and disinformation to further widen societal and political divides," it said in its Global risks report 2024. That fact, that AI-generated misinformation and disinformation ranked top for potential severity over the next couple of years – ahead of extreme weather events – should give all organisations pause for thought. The immediate effect of such tactics could range from civil unrest to an undermining of the legitimacy of newly elected governments. More troubling is that over the

“Emerging as the most severe global risk anticipated over the next two years, foreign and domestic actors alike will leverage misinformation and disinformation

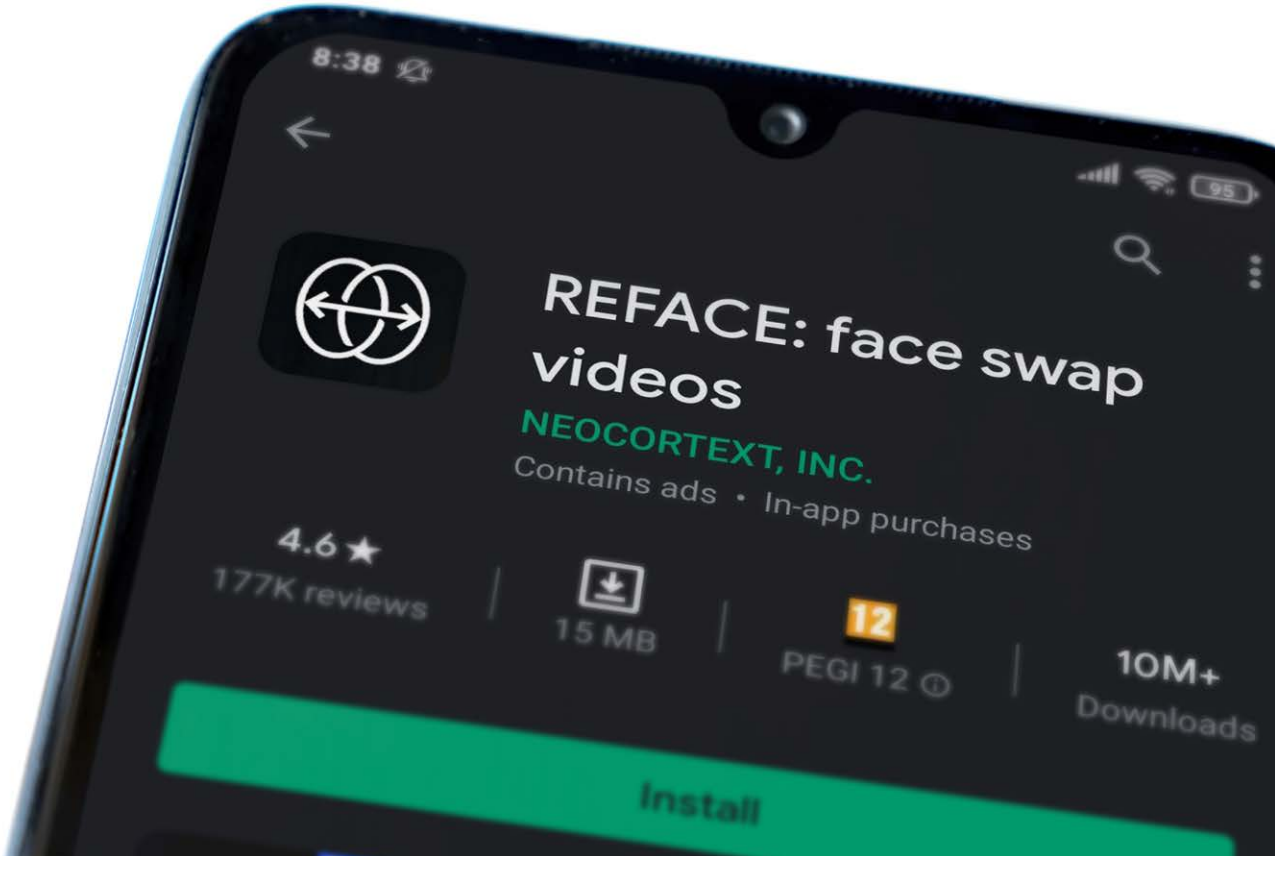


Image credit: Maor_Wine Itob / Shutterstock.com

> **Anyone with a few days to spare and the determination to learn could become proficient enough to create reasonable deepfakes within a week**

longer term the kind of political polarisation that has been fuelled by the tendency of social media algorithms to highlight extreme views will infect public discourse with believable nonsense.

"In response to mis- and disinformation, governments could be increasingly empowered to control information based on what they determine to be 'true'," WEF said. "Freedoms relating to the internet, press and access to wider sources of information that are already in decline risk descending into broader repression of information flows across a wider set of countries."

Easy to create

The creators of the phoney Biden call used technology generally referred to as deepfake – in this case an actor said the words and the audio was distorted to sound like the US president. But working with videos is also possible. The media file in question is altered by deep neural networks to build on the source material in a way that creates a character that closely mimics the original person. The algorithms can copy voice intonation, speech patterns, facial movements and body language to make the final version sometimes indistinguishable from a real recording of that person.

Deepfake terminology and culture emerged from the popular Reddit forum in 2017 – perhaps, unsurprisingly, in the form of pornographic videos. Reddit banned such synthetic technology from its platform, but not before a large, global subculture had gathered around the practice. The development of deepfake has been rapid – and was used by a Belgian political party, the Flemish Socialist Party – in 2018 to create a video of Donald Trump urging voters to follow North America's lead and exit the Paris climate agreement. The video is not particularly good – and the party said that it was not intended to dupe voters but to provoke debate – but wind forward six years to today and it would be easy to create a video that looked, sounded and felt real.

Deepfake software and apps are readily available – from the highly professional DeepFaceLab, to other more prosumer and amateur apps that people use for fun on platforms such as Facebook and TikTok. Yet even scrolling for a few minutes through the internet, it is easy to find simple-to-follow tutorials

TECH ACCORD COMMITMENTS

Participating technology companies agreed to eight specific commitments in order to safeguard forthcoming elections. Those comprise:

- Developing and implementing technology to mitigate risks related to Deceptive AI Election Content, including open-source tools where appropriate
- Assessing models in scope of this Accord to understand the risks they may present regarding Deceptive AI Election Content
- Seeking to detect the distribution of this content on their platforms
- Seeking to appropriately address this content detected on their platforms
- Fostering cross-industry resilience to Deceptive AI Election Content
- Providing transparency to the public regarding how the company addresses it
- Continuing to engage with a diverse set of global civil society organisations and academics
- Supporting efforts to foster public awareness, media literacy and all-of-society re silience

Source: *Microsoft*

on the use of professional-level software that can enable even people who cannot code to create realistic-looking, deepfake representations. Anyone with a few days to spare and the determination to learn could become proficient enough to create reasonable deepfakes within a week. State actors with unlimited resources and expertise can take those techniques to the next level.

Regulating deepfakes

Around the same time that Joe Biden's doppelganger was urging democratic voters to hold fire in New Hampshire, a wave of pornographic images of Taylor Swift swept through X, the social media platform, according to the Guardian newspaper. It reported that one image attracted 47 million views before the platform took it down – and a few days later X removed all images from its site and blocked searches mentioning the celebrity's name.

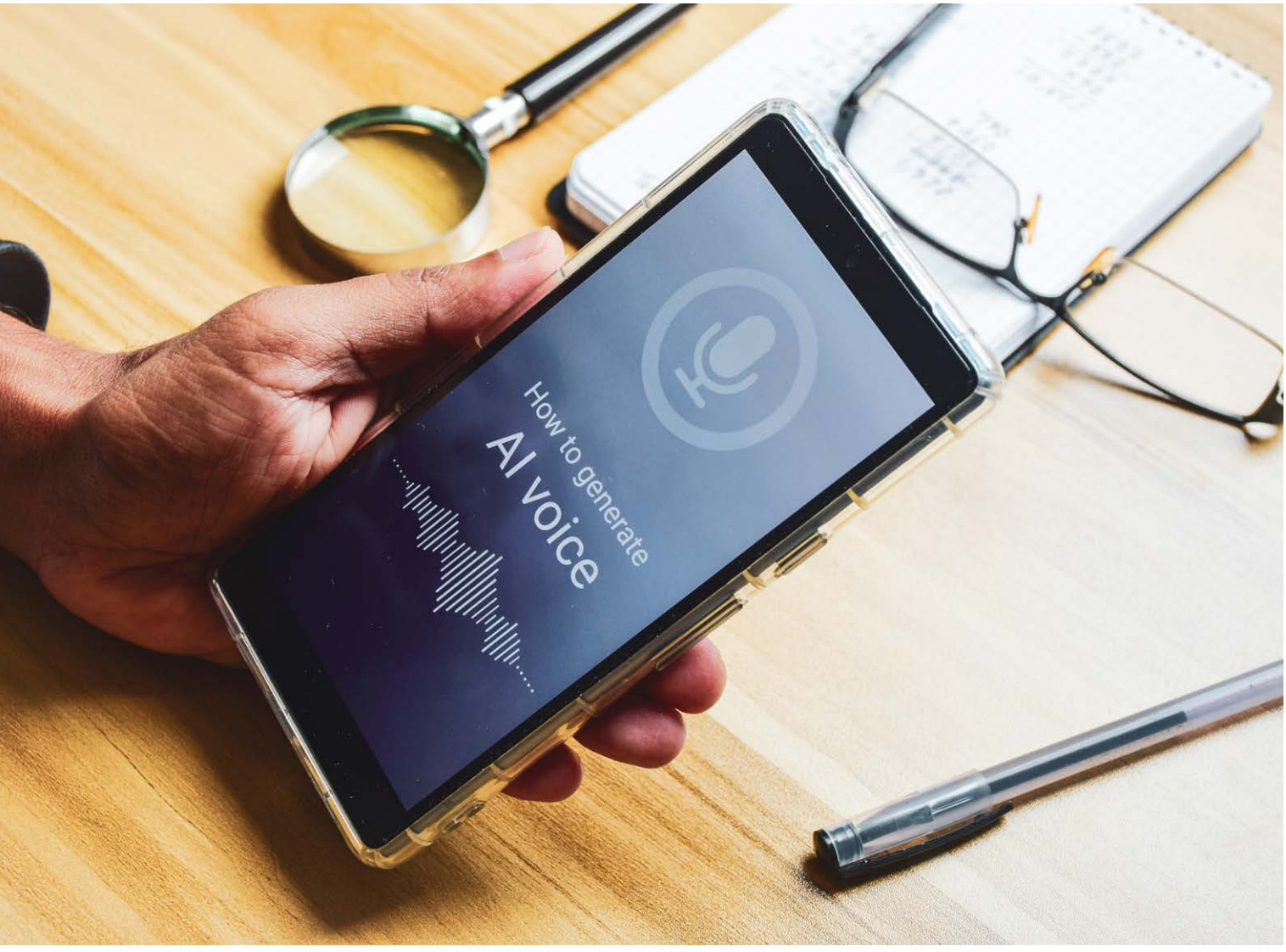
Taylor Swift's legal team is reportedly considering avenues of legal redress. But in the UK, the patchwork of laws that will eventually govern some aspects of deepfakery are still in their infancy. The long-awaited Online Safety Act, for example, received Royal Assent in October 2023. The regulator Ofcom is responsible for implementing the provisions on illegal content and pornography and ensuring that there is a sufficient focus on protecting women and girls from harmful content. But the timelines for developing such protections look glacial compared to how fast events move online.

> **"An estimated 40 per cent of businesses or their customers said that they had encountered deepfake attacks**

In phase one of its programme of work under the Act, for instance, Ofcom is consulting on "codes and guidance relating to dangers online such as terrorism or fraud, as well as protecting children from sexual exploitation and abuse", according to JMW, a law firm with technology expertise. That guidance needs to be ready 18 months after the Act received Royal Assent. But the specific guidance on pornography and content related to self-harm will not be ready until summer 2025. Fines for breaches of those codes could eventually be punishing.

"Ofcom will enforce the codes, and the risk to tech companies are potentially severe," according to JMW partner Dominic Walker. "Ofcom can issue fines of up to £18 million or 10 per cent of their global annual revenue, whichever is bigger. The government has said that fines could potentially reach billions of pounds."

The European Union's forthcoming AI act takes a risk-based approach to all AI that will operate in Europe – with deepfakes falling under its limited risk category. In addition, Europe's Digital Services Act is meant to specifically force social media platforms to combat politically motivated disinformation that is intended to tamper with election results. From late last year, so-called Very Large Online Platforms must publish the indicators used in algorithms that detect hate speech, for example, and they must show how many fact-checkers are employed per national language



> **Twenty leading technology businesses signed up to an industry-devised voluntary code to help prevent fake news influencing upcoming elections**

for member states. The European Commission used the regulations to open infringement proceedings against X late last year.

But the situation in the US is more targeted. In May last year, Joseph Morelle introduced a bill to Congress called Preventing Deepfakes of Intimate Images Act, which amends an existing law relating to violence against women to specifically include deepfakes. Separately this year another initiative – the bipartisan Disrupt Explicit Forged Images and Non-Consensual Edits Act of 2024 (or the DEFIANCE Act of 2024) seeks to hold accountable those who are responsible for the proliferation of non-consensual, sexually explicit deepfakes. Taken together, that would enable victims to go after both creators and distributors.

Given the growing political heat AI-generated fakes are creating, the technology industry has responded. In February 2024, 20 leading technology businesses signed up to an industry-devised voluntary code to help prevent fake news influencing upcoming elections, *Tech accord to combat deceptive use of AI in 2024 elections* (see *Tech accord commitments*). Signatories included Adobe, Amazon, Google, IBM, Meta, Microsoft, OpenAI, TikTok and X.

Business attacks

Deepfakes are also beginning to target businesses. An estimated 40 per cent of businesses or their customers said that they had encountered deepfake attacks in a survey reported by the website Biometric update. In a discussion hosted by the site, participants said that many businesses respond to threats such as identity theft by

US GOVERNMENT'S RECOMMENDED DEFENCES

- **Plan:** Ensure plans are in place among organisational security teams to respond to a variety of deepfake techniques. These should be prioritised by the likelihood and unique vulnerabilities of each organisation and their industry. Some organisations will be more susceptible to executive impersonation or misinformation which may impact brand status or public stock shares. Others relying on high volumes of virtual financial transactions may be more vulnerable to financial fraud.
- **Rehearse:** Once a plan is established, do several tabletop exercises to practise and analyse the execution of the plan. These should involve the most likely targets of deepfakes and include executives who may be prime targets.
- **Report and share experiences:** Report the details of malicious deepfakes with appropriate government partners, to spread awareness of trending malicious techniques and campaigns.
- **Train personnel:** Every organisation should incorporate an overview of deepfake techniques into their training programme. This should include an overview of potential uses of deepfakes designed to cause reputational damage, executive targeting and business email compromise attempts for financial gain, and manipulated media used to undermine hiring or operational meetings for malicious purposes. Employees should be familiar with standard procedures for responding to suspected manipulated media and understand the mechanisms for reporting this activity within their organisation.
- **Leverage cross-industry partnerships:** C2PA is a significant effort launched in 2021 to address the prevalence of misleading information online through the development of technical standards for certifying the provenance of media content.
- **Understand what private companies are doing to preserve the provenance of online content:** Organisations should actively pursue partnerships with media, social media, career networking and similar companies in order to learn more about how these companies are preserving the provenance of online content. This is especially important considering how they may be working to identify and mitigate the harms of synthetic content, which may be used as a means to exploit organisations and their employees.

Source: *US Government*

collecting more customer data – which can increase the risk if not stored securely and heighten the risk of more data breaches.

"Breached data both provides the data attackers need to break through the weak point in businesses' defences, but also fuels the training of deepfakes used in biometric presentation or injection attacks," it said.

Deepfake fraud can be lucrative. Late last year, Dubai police bust a syndicate that had used the technique to syphon $36 million from two Asian companies. In the first attack, the group hacked into the company's email account and intercepted communications between the chief executive officer and branch offices. "Using AI-powered deepfake technology, police said the gang impersonated the company directors and replicated their voices to instruct branch managers to transfer $19 million to a Dubai-based account for a confidential acquisition deal in the emirate," said one account. In another case, a bank in the United Arab Emirates was tricked by an AI voice to pay $35 million.

The US government has provided advice on how businesses can defend themselves against deepfakes (See *US government's recommended defences*). From a risk management perspective, experts have recommended boosting cybersecurity defences by implementing a compliance framework such as ISO27001. That requires conducting a comprehensive information security risk assessment, which pays particular attention to those controls that identify and combat such risks, according to ISMS, an information security business.

While regulators and businesses move fast to stem the impact of the rise of these synthetic doubles, the fakers are hard at work making them better and easier to create and disseminate. It is hard to imagine businesses and political systems being able to stop the tide in the immediate future – especially since similar responses to online harms, for example, have so far suffered from protracted development. There may come a time when it will be necessary to assume that everything is fake unless proven otherwise. Perhaps that time has already come.

Improvement in action

BY TOM CLARE

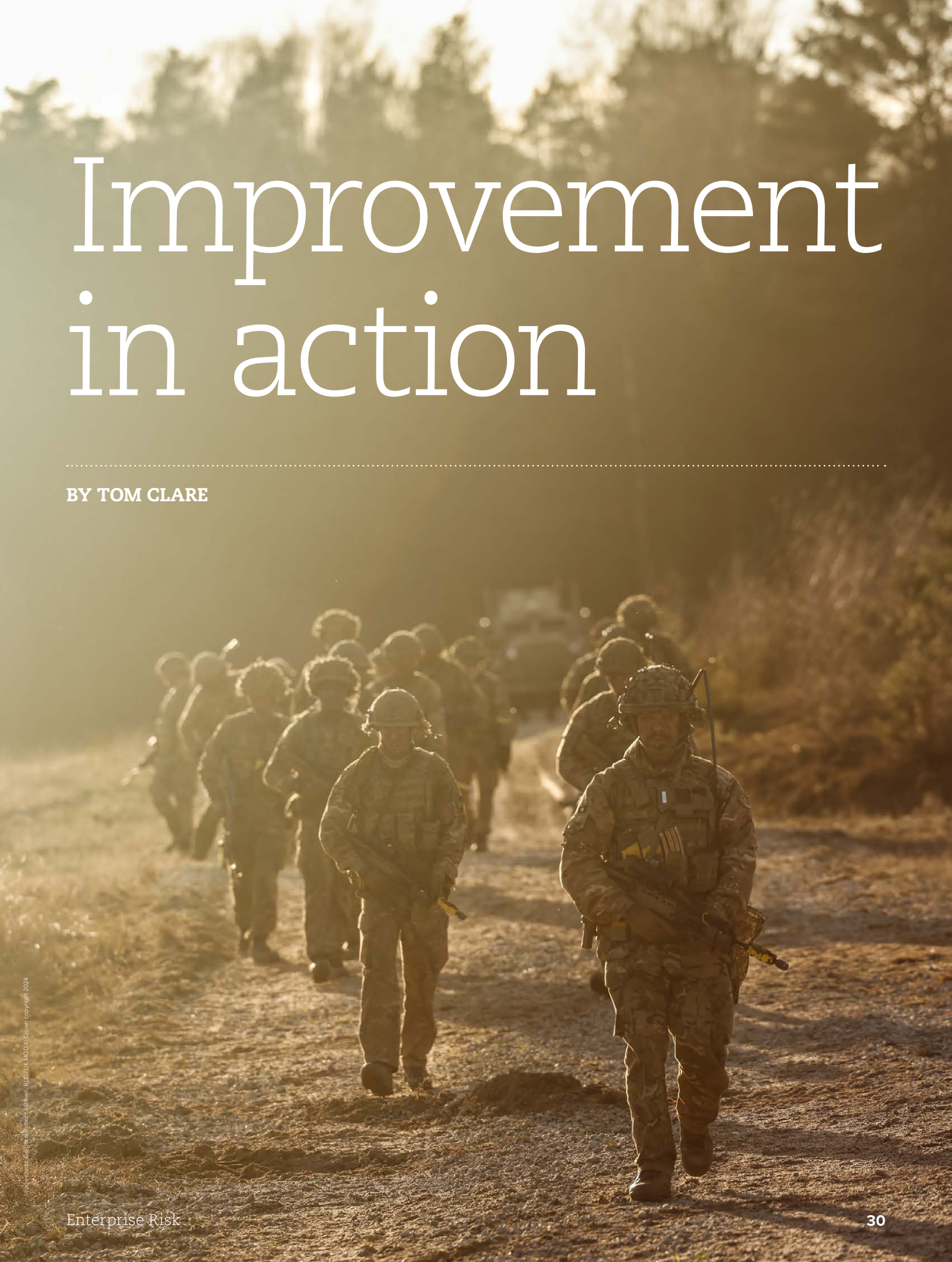


Image credit: Cpl Rebecca Brown, RLC/UK MOD © Crown copyright 2024

Risk professionals are meant to enhance their processes and link them to the strategic direction of the business. But what does that mean in practice?

Defence Equipment and Support (DE&S) is a highly specialised part of the Ministry of Defence. From the procurement of clothes, carriers and rations to rifles, we ensure the UK armed forces – the Royal Navy, the British Army and the Royal Air Force – have the equipment and support they need to carry out their duties. Operating with an annual budget of around £10 billion, we have an active risk management community of around 100 risk managers to support the delivery of these complex projects, programmes and portfolios of work.

To ensure we are providing the best possible service to deliver our complex remit in a rapidly changing world, our risk management function has been engaged in a risk improvement programme over the past year.

As a profession, we are often faced with the challenge to improve or show risk can be done better. How can you go about it? In challenging economic times, the need to highlight the value of what a risk function can bring is vital – what could we do to make such changes? We identified five workstreams to focus on that we believe were key to our recent success at the Continuity Insurance and Risk Magazine awards in November 2023: leadership and management, risk strategy and policy, risk culture and behaviours, risk handling and assurance, and risk outcomes and delivery.

Leadership and management

We made several changes to the leadership and management structure. The organisation appointed our deputy chief executive our risk champion. He is there as a senior and visible leader across DE&S to advocate for improvements to risk at all levels of the business, champion the specialism and communicate progress and areas of interest in progress on risk to the wider business. Our non-executive directors are now working alongside the risk owners on the board, providing external and independent challenge to ensure there are effective risk response plans in place. Lastly, we put in place a risk lead for the specialism, to better cohere the progress and development of risk as a profession in the business and to provide leadership and guidance to the risk community.

> **“ As a profession, we are often faced with the challenge to improve or show risk can be done better**

How could this apply to your organisation? First, consider who is championing risk management. Is there a senior leader within the executive who has expressed an interest in risk management and in making sure it is done effectively? A conversation with them could provide a powerful ally for you to improve how risk is seen across the organisation and help set the right tone at the top.

Second, is the governance structure that is in place being used to its best effect? Are there non-executive directors or similar in your organisation who could help? Can a conversation be had to bring the benefit of independent challenge into the risk process – through working alongside risk owners or by asking for periodic deep dives to be part of the board-level agenda.

Finally, do you have a leader for the risk profession? If you have several risk managers in your business, who is acting in the second-line capacity who can help cohere process, policy and procedures, and ensure risk is working in line with the strategic direction of the organisation?

Risk strategy and policy

We have enhanced our existing suite of processes and procedures to assist our risk management community in their role, including creating consistent ways of working in our risk software, improved guidance and the establishment of new processes. We have also completed a full refresh of the organisation’s risk policy, which has been endorsed by our risk champion and finance director. This sets out how our

“Who is acting in the second-line capacity who can help cohere process, policy and procedures, and ensure risk is working in line with the strategic direction of the organisation?

project teams can escalate risks at the senior governance levels, ultimately taking matters to the attention of the board, if required. By clearly setting out the risk framework we will operate, we have enhanced the understanding of risk across the business, with escalation routes in place to enable a project-level risk to become a board-level risk if it was required.

It is worth considering refreshing or formalising your risk processes. Being clear on what the process is will provide clarity about the organisation's approach and important guidance for users to refer to. This does not need to be a vast document. It should be proportional to your organisation and the context within which you are operating. But the clarity that comes from enhancing those processes can strongly contribute to a common understanding of why the risk managers are there, what they will do for the business and how the structure will operate.

Risk culture and behaviours

It was crucial to communicate those changes properly across the organisation. We developed several in-house training products to raise awareness across the business of risk. These are designed for everyone, not just for our risk professionals. They include an introductory course called *Get to know risk management*, and a *Fundamentals* course, which provides a more detailed overview. This is key to spreading the message that risk is everyone's responsibility, and not just for our risk managers.

We have also made a commitment to investing in our risk managers. Alongside the development of an internal *Practitioner* training course, the Association for Project Management Risk qualifications have been offered to all our risk managers, with a cadre benefiting from the IRM's International Certificate in Enterprise Risk Management – with support and mentoring provided from colleagues who have previously studied for the qualification.

In parallel to the training opportunities, we have worked to ensure there are multiple opportunities for our risk community to come together and learn from each other. Facilitated by a senior risk lead, we established monthly “communities of interest” meetings across our business areas to provide a forum to discuss specific concerns to their areas and to understand new guidance or ways of working.

An annual get-together of the entire risk community provides an additional networking opportunity, a chance to learn about the direction of risk in that year and, most importantly, to celebrate our achievements. Along with a mix of speakers to raise awareness of different areas and offer an external perspective, it helps develop a sense of community within our profession.

The senior risk managers meet regularly in conjunction with the risk lead. This provides an opportunity to discuss risk improvement work, but also fosters a strong tone from the top that we are all working consistently and finding new ways to improve. Key to this improvement work has also been to involve our key internal customer, the project management community. That has helped ensure that our risk managers are providing a service that is

Image credit: LPhot Belinda Alker / UK MOD © Crown copyright 2024

benefiting our key stakeholders.

Finally, we have reached out to the broader government risk management community. In developing a strong relationship with the Government Risk Profession, we have had the opportunity to contribute to improvement work across the government, build professional networks and keep our finger on the pulse of the direction of risk, which in turn helps us plan our future risk improvement work.

This work across the risk community is helping our risk approach become more consistent and pan-DE&S, rather than allowing individual business areas to engage in a patchwork of approaches. In your organisation, it is important for risk managers to be the risk advocate. To help with this process, identify potential gaps where you can develop and deliver awareness courses on risk management. Make something specific, engaging and relevant to your organisation. If funding allows, consider formalising learning through the variety of academic qualifications available. Not only does this provide a boost to your risk managers' development, but it also enhances the professional credibility of those you have in place.

> **“ It is important for risk managers to be the risk advocate**

Just as importantly, ensure you're working with your customers to meet their needs. Seek feedback about the service you or your risk team is providing to the organisation and involve them in any improvement activities. This will help build relationships, provide a more effective service for their needs and improve engagement across the process.

Lastly, ask if there is anyone else out there. If you are one of many risk professionals in your organisation, are there opportunities to meet up, share ideas and learn from each other? If not, create a forum where this can happen. If you are operating by yourself, consider the range of IRM Special Interest Groups out there and use them as a chance to learn from others.

Risk handling and assurance

Our specialism has developed and released a Risk Management Maturity Assessment tool, which feeds into a wider Project Maturity Model. This assessment used among the delivery teams aims to identify key areas of success and areas for improvement within risk management as part of the overall project management process in delivery teams across the organisation. Consider utilising maturity tools or other industry guidance. Baseline where your organisation is at. Be open and honest, and genuinely reflect on how you feel risk is performing in your organisation. A whole range of models are out there; research

Image credit: Corporal Rebecca Brown, RLC / UK MOD © Crown copyright 2024

Image credit: LPhot Belinda Alker / UK MOD © Crown copyright 2024

what might be appropriate for your organisation and conduct the activity. It's likely to provide you with an excellent framework as to where you can target your activity or get the conversation moving.

Outcomes and delivery

We implemented consistent management information dashboards across the organisation to help us harness and understand the huge amounts of valuable risk data present in the business. Utilising the skills of the management information team helped us put in place a consistent way of reporting on the status of risks so that decision-makers can become quickly familiar with what is being put in place. One important lesson has been to focus on data quality. Link the requirements of what you expect from risk management regarding what information is needed, when or how often things should be reviewed and what other detail is needed – then track it. Trends or patterns may emerge within your data that could spark targeted risk improvement activities, be it training on process, your risk tools or engagement with the process in particular areas.

We also made better use of visualisations in our risk reviews, utilising waterfall charts in our board-level discussions to better focus these discussions on the progress of the risk response plan in a clearer way. It is important to consider what you present to decision-makers. Does each unit present risk reports in different styles and approaches? If so, decision-makers must spend their time learning to interrogate your reports rather than having focused discussions. Use consistent reports where possible to ensure familiarity can develop with risk information and they can quickly understand what you wish to put across.

Be creative with the way you present risk to your organisation. Leaders in any organisation have packed calendars and are presented with multiple decisions to make, problems they need to solve and directions to give. Are there visualisations you can make that show the journey of the expected progress of a risk, rather than reams of paper explaining it? Remember that you are the specialist in risk management – take the vast wealth of data, provide the analysis, synthesise it and clearly show the decision or discussion you need management to have to progress with the risk process. Your leadership group are likely to thank you for it with better engagement in the process for next time.

Improvement takes an enduring commitment from all levels, but our approach has yielded results. We have seen a rise in engagement of our risk managers in workplace surveys, more risks are being escalated for appropriate discussion and there has been a significant reduction in late risk reviews. There will always be new areas to explore, further improving the use of tools or techniques, or greater integration of quantitative analysis to support everyday decision-making. Our approach was for a major project management organisation in the public sector, but we believe this can be taken and adapted to an organisation of any size. We will continue to embed, develop and evolve these improvements to ensure we are maximising our contribution to the success of the organisation, and we hope this can inspire positive change in how risk is seen in yours. ER

> **Improvement takes an enduring commitment from all levels**

Tom Clare, CFIRM, is a senior risk manager for Defence Equipment & Support, an organisation within the UK Ministry of Defence responsible for procuring and supporting defence equipment for the UK armed forces. For further information on this organisation, please visit www.des.mod.uk.

Build your career as a risk professional

Training with the IRM

With training courses covering a wide range of enterprise risk management topics, our courses are delivered by industry experts so you can immediately apply the latest in best practice techniques. As well as being practical and interactive, the courses allow you to log CPD hours and some offer accreditation.

Scan me!

www.theirm.org | Tel: +44 (0)20 7709 9808 | Email: enquiries@theirm.org

irm

Directory

Change tomorrow with industry leading GRC software

With powerful, agile and integrated solutions in governance, risk, compliance and strategy, Camms' business software will help you make the right decisions, manage risks and focus on what matters. Working with tens of thousands of users at organisations across five continents, and with over 25 years of experience, Camms thrive on watching their clients achieve results and stay a step ahead. Helping firms meet goals, influences business decisions and board strategy is in Camms' DNA. To learn more, visit www.cammsgroup.com.

Daniel Kandola
+44 (0) 161 711 0564
sales@cammsgroup.com
www.cammsgroup.com
Suite 4.3, Parsonage Chambers
3 The Parsonage
Manchester, M3 2HW
United Kingdom

Cost-effective technology for risk & compliance professionals

1RS provide cutting edge 1RS ERIC (Risk & Compliance), 1RS CASS and 1RS SMCR solutions, which have been designed and built by Risk and Compliance professionals with over 25 years of experience. Our solutions are supported by experts, and we continually update the products to reflect best practice and changes in regulatory expectations. We are trusted by banks, vehicle finance, wealth management, investment banking and management, brokers, and more throughout the United Kingdom and Europe. For more information, visit https://1rs.io

Andrew Firth
+44 (0) 20 7175 6177
hello@1rs.io
1rs.io
38 Borough High Street
London
SE1 2AL

Enterprise risk management and risk analysis software

riskHive are an established global provider of professional cloud, intranet and desktop solutions for the management and analysis of RAID (risks, issues, assumptions and dependencies). Being low maintenance, highly configurable and cloud based, the Enterprise Risk Manager application can get you online in under 24 hours, supporting your existing processes and terminology. Easily import existing risk information to quickly produce a consolidated risk portfolio. Relied on by customers ranging from New Zealand through the Middle East to Northern Europe riskHive deliver a truly global ERM solution with a truly enterprise 'all-in' licence.

Ian Baker or Doug Oldfield
+44 (0) 1275 545874
ian.baker@riskhive.com
doug.oldfield@riskhive.com
www.riskhive.com
riskHive Software Services Ltd.
Dilkush, Farlers End
Bristol, BS48 4PG

To advertise here contact: Redactive Media IRMsales@redactive.co.uk +44(0)20 7324 2753

Risk, audit & compliance software

Symbiant is a market leading provider of Risk, Audit & Compliance software. They have a full range of modules that can be connected for a wholistic view. Customise your own layouts and reports or use the ready-made options. All modules are a fixed £100 per month. Contracts are only 30 day. Visit the website to watch the quick overview videos or to arrange a no obligation web demonstration.

Mark Long
+44 (0) 20 8895 6410
irm@symbiant.co.uk
www.symbiant.co.uk
20-22 Wenlock Road
London
N1 7GU

Risk management software

Since 2014, Origami Risk is the only company that has been consistently recognised for delivering client success, innovation, and stability, while bringing new ideas and advanced features to the RMIS market. Origami Risk's innovative software is designed with the latest technology and a focus on performance and ease-of-use, providing integrated solutions to the entire insurance value chain, serving Risk Managers, Brokers, TPAs and Carriers. It features powerful workflow, advanced reporting and analysis tools, and intuitive features to improve productivity and better manage total cost of risk—saving our clients time and money and enabling them to be more successful. Learn more at www.origamirisk.com

Neil Scotcher
+44 (0) 16179 17740
nscotcher@origamirisk.com
www.origamirisk.com
30 Moorgate
London
EC2R 6PJ

Risk management software

In today's rapidly evolving world, business models and organisations are facing increased change and unprecedented levels of scrutiny. With change comes complexity, challenging risk managers to redefine the way they lead an organisation's approach to and implementation of risk management. Protecht helps organisations through deep understanding, monitoring and management of risk. We provide the complete risk solution—comprised of world-class enterprise risk management, compliance, training and advisory services—to government organisations, key regulators and businesses of all sizes across the world. With 20+ years at the forefront of risk and compliance solutions, millions of incidents managed across thousands of individual risks, and over 25 thousand people attending our training courses to date, we're one of the most respected and influential voices in risk.

N/A
+44 (0) 20 3978 1360
info@protechtgroup.com
www.protechtgroup.com
77 New Cavendish Street
The Harley Building
London W1W 6XB
United Kingdom

To advertise here contact: Redactive Media IRMsales@redactive.co.uk +44(0)20 7324 2753

Lessons from Spinoza

As work becomes increasingly infected with pointless activities, organisations need to act to improve worker engagement

When the late anthropologist David Graeber argued that many employees believed their jobs served no social purpose in the radical magazine *Strike!* back in 2013, the claim hit a raw nerve. Not only did the piece go viral globally, but he was inundated with stories from disgruntled employees sharing their despair.

"I contribute nothing to this world and am utterly miserable all of the time," confessed one corporate lawyer – a tax litigator – Graeber reported in his 2018 best-selling book *Bullshit jobs: the rise of pointless work and what we can do about it.*

While pundits often believe that pointless jobs predominantly exist in the public sector, Graeber argued that, in an age of relentless sub-contracting, many of those roles are actually performed by white-collar staff working in the private sector. The most glorious example did, however, involve a Spanish civil servant who skipped work at Aguas de Cádiz for six years on full pay and became an expert in the thought of the Spanish philosopher Baruch Spinoza. His clandestine studies only emerged when managers could not find the

absent engineer to present him with a medal for long service.

Mission creep

A recent statistical study by Simon Walo, a researcher at Zurich University, showed that ennui does indeed reign particularly strongly among those working in finance, sales and managerial roles – especially in the private sector. Yet the mission creep of bullshit-style activities is perhaps more concerning. A study by the researcher Gallup found that less than a quarter of employees say they are "engaged with work", costing an estimated hit to global GDP of 9 per cent. Wasteful meetings, pointless admin and, increasingly, being bombarded by messenger apps, means that knowledge workers spend only 18 per cent of their time on directly productive activity, according to Zapier.

In his study, Walo decided to see whether people felt particularly disengaged when doing boring, repetitive work. Those are the kinds of tasks management consultants – workers that Graeber felt generally fitted his derogatory category – have often labelled as being ripe for automation. But while routine work was sometimes cited as a cause for dissatisfaction by those in enforced drudgery, "the nature of the job still had a large effect beyond those factors", Walo concluded. So, while AI and other automation processes can help, they do not strike at the heart of the problem.

What can organisations do? One obvious way to meet this challenge head-on is to ask workers a specific question – such as, on a scale of 1 to 5, how far do you feel your role has a social purpose? Could those people be trained, for example, so that they are able to split their time between the "useless" tasks and those that they perceived have more value? Crucially, since engagement is so central to productivity, perhaps organisations should listen to the wise words of Spinoza himself when he says, "I have striven not to laugh at human actions, not to weep at them, nor to hate them, but to understand them."

"A Spanish civil servant skipped work at Aguas de Cádiz for six years on full pay and became an expert in the work of the Spanish philosopher Baruch Spinoza

Do you manage risk in your organisation?

Get risk ready with the IRM

There has never been a better time to increase your earning potential and career prospects by gaining an internationally recognised risk management qualification.

Scan me!

a.r.u. | Anglia Ruskin University · EDINBVRGH THE CITY OF EDINBURGH COUNCIL · Gateshead Council · NHS · Norfolk County Council · The Open University

www.theirm.org | Tel: +44 (0)20 7709 9808 | Email: enquiries@theirm.org

irm